



FEB 3 1998

Washington, D.C. 20530

Mr. Thomas Wheeler  
President and CEO  
Cellular Telecommunications Industry Association  
1250 Connecticut Avenue, NW, Suite 200  
Washington, DC 20036

Dear Mr. Wheeler:

This letter confirms discussions held between the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and representatives of the telecommunications industry during a January 23, 1998, meeting<sup>1</sup> regarding DOJ's position on the legal status under the Communications Assistance for Law Enforcement Act (CALEA) of the 11 electronic surveillance capabilities (referred to as the "punch list") that are missing from the current Telecommunications Industry Association (TIA) electronic surveillance standard J-STD-025. Additionally, it confirms the terms and conditions upon which DOJ will forbear bringing enforcement actions against industry members for non-compliance with CALEA.

**"Punch List"**

DOJ has reviewed the 11 "punch list" capabilities in reference to CALEA, its legislative history, and the underlying electronic surveillance statutes<sup>2</sup>. In addition, DOJ reviewed a memorandum evaluating the "punch list" under CALEA that was prepared by the Office of General Counsel (OGC) of the FBI. As a result of its review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within

---

<sup>1</sup>Those in attendance at the January 23, 1998, meeting included representatives from the Cellular Telecommunications Industry Association (CTIA), Personal Communications Industry Association (PCIA), Telecommunications Industry Association (TIA), United States Telephone Association (USTA), Bell Atlantic, Department of Justice and the Federal Bureau of Investigation.

<sup>2</sup> CALEA was enacted to preserve the electronic surveillance capabilities of law enforcement commensurate with the legal authority found in the underlying electronic surveillance statutes, and so that electronic surveillance efforts could be conducted properly pursuant to these statutes.

review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within the scope of CALEA and the underlying electronic surveillance statutes. These nine capabilities are<sup>3</sup>:

- Content of conferenced calls;
- Party Hold, Party Join, Party Drop;
- Access to subject-initiated dialing and signaling
- Notification Message (in-band and out-of-band signaling);
- Timing to correlate call data and call content;
- Surveillance Status Message;
- Feature Status Message;
- Continuity Check; and
- Post cut-through dialing and signaling.

With respect to the first four capabilities (Content of conferenced calls; Party Hold, Party Join, Party Drop; Access to subject-initiated dialing and signaling; and Notification Message of in-band and out-of-band signaling), DOJ firmly believes that law enforcement's analysis and position regarding these assistance capability requirements satisfy CALEA section 103 requirements. These descriptions are set forth in the response submitted by the FBI<sup>4</sup> to TIA Committee TR45.2 during the balloting process on standards document SP-3580A.

With respect to the fifth through the ninth capabilities (Timing to correlate call data and call content; Surveillance Status Message; Feature Status Message; Continuity Check; and Post cut-through dialing and signaling), DOJ has also concluded that law enforcement's position satisfies CALEA section 103 requirements. Because of this opinion, discussion between the industry and law enforcement will be required in order to select a mutually acceptable means of delivering the information specified by each capability. Thus, if industry disagrees with law enforcement's proposed delivery method, it must affirmatively propose a meaningful and effective alternative.

Based upon the foregoing analysis, it is DOJ's opinion that TIA interim standard J-STD-025 is failing to include and properly address the nine capabilities listed above. Industry and law enforcement may wish to act in concert to revise the interim standard J-STD-025 to include solutions for each of these missing electronic surveillance capabilities.

---

<sup>3</sup> See Items 1-7, 9, and 10 of Attachment A.

<sup>4</sup> The FBI is closely coordinating its efforts with state and local law enforcement representatives across the nation. In this document "law enforcement" and "FBI" refer to this partnership and are used interchangeably.

With respect to capability number eight (Standardized Delivery Interface), although a single delivery interface is not mandated by CALEA, DOJ believes that a single, standard interface would be cost effective and of great benefit to both law enforcement and telecommunications carriers. Recent productive discussions with industry have resulted in what DOJ believes is an acceptable compromise, whereby the industry would commit to a limited number of no more than five delivery interfaces. DOJ supports such an agreement.

With respect to capability number 11 (Separated Delivery), DOJ, while recognizing the usefulness of such delivery for the effectiveness of electronic surveillance, nevertheless does not believe that CALEA section 103, or the underlying electronic surveillance statutes, require separated delivery.

Building on the progress made during the final months of 1997, the FBI's CALEA Implementation Section (CIS) will continue to work with solution providers<sup>5</sup> to reach an agreement on the technical feasibility of all the CALEA capability requirements.

#### **Forbearance**

During the January 23, 1998, meeting, the parties discussed the conditions under which DOJ would agree not to pursue enforcement actions against the carrier under section 108 of CALEA with regard to the CALEA mandate that a carrier meet the assistance capability requirements pursuant to CALEA section 103 by October 25, 1998, or against a manufacturer with respect to its obligation under CALEA section 106(b) to make features or modifications available on a "reasonably timely basis." A letter from the Office of the Attorney General, which was provided to all meeting attendees, outlined the basic conditions regarding forbearance:

In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, DOJ will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. DOJ

---

<sup>5</sup> Solutions providers include not only switch-based manufacturers, and support service providers, but other industry entities that are engaged in the development of network-based and other CALEA-compliant solutions.

will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement.

DOJ, in consultation with the FBI, has further elaborated on the conditions related to forbearance as follows:

Any member of the telecommunications industry seeking forbearance must submit to CIS a statement that identifies the following:

1. The CALEA capability requirements that will be included in its platform or designed into any non-switch-based solution.
2. The projected date by which the platform, or non-switch-based solution, will be made commercially available, the "commercially available date."
3. A timeline for design, development, and testing milestones that will be achieved by the manufacturer from the start of the project through the commercially available date, the "milestone timeline."
4. A schedule for furnishing information to CIS at each milestone to permit CIS to verify that a milestone has been reached.
5. A list of specific types of information to be provided according to the foregoing schedule.
6. A schedule for providing mutually agreed upon data to CIS from which the Government will be able to determine the fairness and reasonableness of the CALEA solution price.
7. A list of the specific types of price-related data to be provided.

With respect to item 1, the term "CALEA capability requirements" refers to the functions defined in the TIA interim standard J-STD-025 and the first nine punch list capabilities described earlier in this letter. Law enforcement will work with each solution provider as it produces a technical feasibility study to confirm its understanding of, and ability to meet, the CALEA capability requirements. For those switching platforms, or non-switch-based solutions, on which a capability is technically infeasible, law enforcement will consult with solution provider to assess the possibility of providing effective technical alternatives that will still provide law enforcement with the necessary evidentiary and minimization data sought by the capability.

With respect to item 2, the term "commercially available date" refers to the date when the platform or non-switch-based solution

will be made available by the solution provider for the immediate purchase and deployment by a carrier. That date shall, in no event, extend beyond the first currently scheduled software generic product release after the October 25, 1998, capability compliance date. With respect to item 3, the term "milestone timeline" refers to a schedule of the necessary design, development, and testing steps to be taken by a solution provider in making a product commercially available. With respect to item 4, a solution provider is expected to include a schedule specifying the time after the completion of each milestone when CIS will be able to verify that the milestone has been reached. With respect to item 5, the specific types of information contained in the affirmative confirmation of the foregoing schedule will include, but not be limited to, draft design documents, feature specification documents, and test results. With respect to item 6, a solution provider is expected to provide a schedule detailing the delivery to CIS of all necessary information for the government to make a determination of the fairness and reasonableness of the price of the solution provider's commercially available CALEA solution. With respect to item 7, the specific types of information contained in the price-related information of the foregoing schedule will include but not be limited to, market prices of comparable features with similar levels of design, development, and testing effort.

Forbearance for a solution provider, and its carrier customers, will be conditioned upon its ability to provide the above listed items as well as to meet verifiable solution development milestones. A solution provider's failure to meet these milestones will result in the loss of forbearance for the solution provider.

Carrier forbearance ends with the commercial availability of a solution. Switches, or portions of a network, of historical importance to law enforcement for which the government must reimburse the carrier will be identified by CIS. Equipment, facilities, and services installed or deployed after January 1, 1995, will be included in any forbearance until a solution is commercially available. Following solution availability, for those switches or portions of a network not identified by CIS, carriers are expected to follow their normal deployment process in determining which switches, or portions of their networks, will be upgraded with the CALEA capabilities. Figure 1 illustrates the basic elements of forbearance.

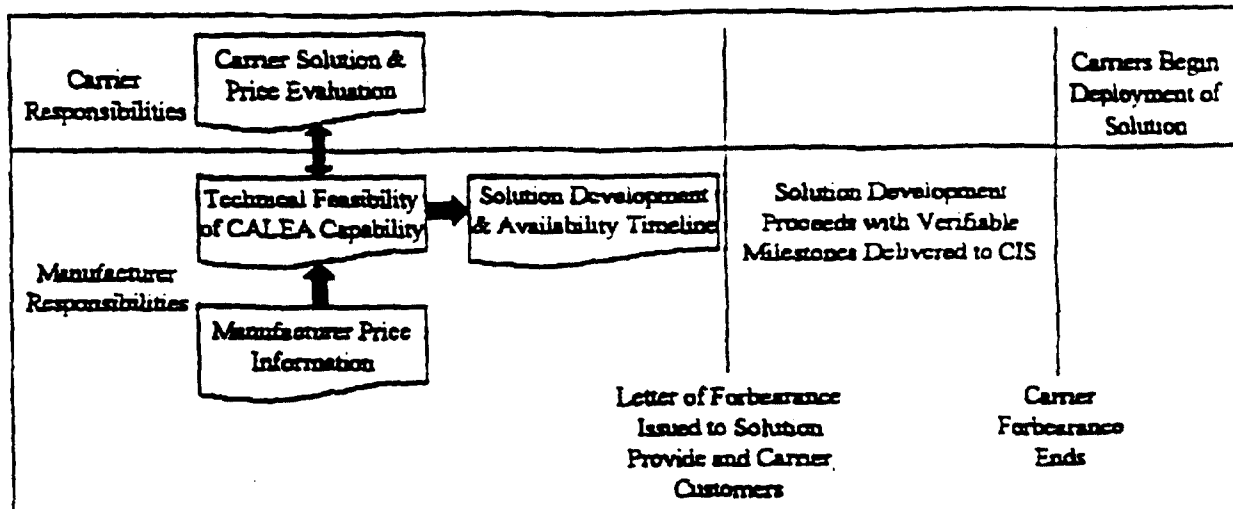


Figure 1: Forbearance

The foregoing forbearance discussion centers on two separate and distinct agreements: Agreements in Principle (AIP) between the FBI and a solution provider, and Cooperative Agreements between the FBI and a carrier.

In an AIP, the FBI and solution providers agree that solution providers have complied with the seven criteria listed above, including a feasibility analysis and pricing information for CALEA capability requirements. The feasibility analysis and pricing information will allow the government to finalize its position regarding the standard, extension of the compliance dates, forbearance, etc. The FBI, in consultation with law enforcement, will not be in a position to make critical determinations until the information described in the above seven criteria has been provided.

Currently many versions of draft AIPs are circulating, both FBI and industry-generated, and some are more comprehensive than is presently warranted. Some of the AIPs in circulation were derived from an AIP drafted by TIA. The FBI hopes to meet with TIA during the week of February 2, 1998, to discuss the proposed AIP. The results of these discussions will then be disseminated to TIA's membership and any other interested solution provider.

The Cooperative Agreement, on the other hand, is the contractual vehicle whereby telecommunications carriers will receive reimbursement for their eligible CALEA costs. Cooperative Agreements may be executed for different purposes at different stages of CALEA implementation. For example, an initial round Cooperative Agreement negotiations is taking place to establish contractual vehicles whereby carriers selected to support specific solution providers with the feasibility analyses and pricing information may receive reimbursement for assisting in

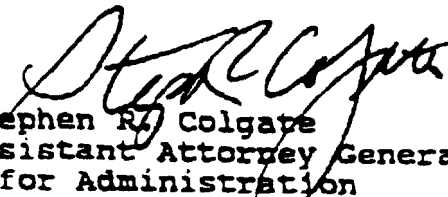
7

this effort. Unfortunately, this initial round of negotiations has encountered some problems. One of the issues is the clarification of a carrier's role in assisting in the analysis of the solution provider's proposed solution. It appears from discussions with carriers that a mutual understanding of the intent of the government's proposed language for the Cooperative Agreements and its Statement of Work (SOW) does not yet exist. Carriers commented that the SOW included a consultative role that the carriers are unable or unwilling to perform. Although it was the government's intent to construct an SOW flexible enough to allow carriers to accommodate their normal roles in the solution provider product development process, the proposals received in response to the SOW have been too non-specific to provide real value.

The FBI still believes, and has had it confirmed by solution providers, that carriers have an essential role to play in developing the CALEA solution. The FBI will now request that each solution provider describe in detail the typical interaction it might have with one of its carrier customers during new product development. These descriptions will then be incorporated into the proposed SOWs, which the government will seek from carriers.

Your continued willingness to work with law enforcement toward the development of electronic surveillance solutions is greatly appreciated.

Sincerely,

  
Stephen R. Colgate  
Assistant Attorney General  
for Administration

# ATTACHMENT A

## BRIEF DESCRIPTION OF PUNCH-LIST CAPABILITIES

Number	Name	Description
1	Content of subject-initiated conference calls	Capability would enable law enforcement access content of conference calls supported by the subject's service (including the call content of parties on hold).
2	Party Hold, Join, Drop	Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined or has been dropped from the conference.
3	Access to subject-initiated dialing and signaling	Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features. (Examples include the use of flash-hook, and of feature keys.)
4	In-band and out-of-band signaling (Notification Message)	A message would be sent to law enforcement when subject's service sends a tone or other network message to the subject or associate. This can include notification that a line is ringing or
5	Timing to associate call data to content	Information necessary to correlate call identification information with the call content of a communications interception.
6	Surveillance Status Message	Message that would provide the verification that interception is still functioning on the appropriate subject.
7	Continuity Check (C-Tone)	Electronic signal that would alert law enforcement if the facility used for delivery of call content interception has failed or lost continuity.
8	Standardized delivery interface	Would limit the number of potential delivery interfaces law enforcement would need to access from the industry.
9	Feature Status Message	Message would provide affirmative notification of any change in a subject's subscribed-to features.
10	Post cut-through dialing and signaling	Information would include those digits dialed by subject after the initial call setup is complete.
11	Separated delivery	Each party to a communication would be delivered separately to law enforcement, without combining the voices of an intercepted (conference) call.





# The Wiretap Act of 1994

Primer for complying with  
the Communications  
Assistance for  
Law Enforcement Act,  
Public Law 103-414



Building The  
Wireless Future

CTIA

Cellular  
Telecommunications  
Industry Association

## I. Introduction

FOR MANY YEARS, THE FEDERAL BUREAU OF INVESTIGATION sought without success to convince Congress to impose broad government-mandated technological requirements on the equipment, facilities, and services of all telecommunications carriers, including wireless systems, to facilitate law enforcement's wire and electronic surveillance capability. In support of these efforts, federal, state, and local law enforcement agencies cited the increasing number of wiretap orders directed at all users of wireless services, particularly in large metropolitan areas, and limited availability of ports on many cellular carriers' systems. In addition, the FBI sought assurances that new and advanced technologies would not inhibit lawful surveillance activities.

Finally, on October 7, 1994, after lengthy debate and intense negotiations with all segments of the communications industry the 103rd Congress completed action on H.R. 4922, the "Communications Assistance for Law Enforcement Act." The Act details a telecommunications carrier's obligation to cooperate in the interception of communications for law enforcement purposes. The act was signed by President Clinton on October 25, 1994, and became Public Law 103-414.

The law attempts to strike a balance between law enforcement needs and industry concerns. During the course of the legislative debate, Congress heard repeatedly from law enforcement, represented primarily by the FBI, that advances in digital technology and the introduction of new intelligent network services, such as call-forwarding, and Follow-Me roaming, were disabling the traditional wiretap capabilities of law enforcement. Industry representatives expressed concern over uncertainties as to liability, cost, and vague reimbursement obligations. Congress noted its concern over the potential for government mandates to dictate how

private companies could research, develop, and deploy telecommunications services and products.

Up until final passage, the political agenda revolved around seemingly endless attempts to specify in legislative language the exact obligations carriers would be held to, how carrier compliance would be determined, and exactly how much and over what time period Congress would appropriate federal funds to reimburse carriers.

This primer has been prepared to provide CTIA member companies with a comprehensive analysis of the wiretap law, detailing the specific obligations imposed on carriers, manufacturers, and support service providers, along with the reimbursement procedures to be followed by both the government and the industry.

### A. CTIA'S FIVE-POINT WIRETAP POSITION

AT ITS MARCH 1994 MEETING, THE CTIA BOARD OF DIRECTORS ADOPTED a five-point position regarding the proposed wiretap legislation. The enacted law contains provisions addressing all five points identified by the Board:

- It includes language that makes illegal the cloning of wireless phones and the ownership of equipment to alter or modify wireless phones;
- It requires that all wireless systems shall have sufficient wiretap capacity, but that the determination of sufficient capacity will be subject to a notice and comment procedure, and recognizes that capacity demands are not uniform across all wireless markets;
- It provides that the government will reimburse carriers for the cost of upgrades necessary to achieve compliance with the Act's requirements;
- It establishes that the appropriate point in a wireless system for a legal wiretap is at the switch and that, as to roamers, wireless carriers are only required to provide information identifying the carrier within whose system a target is roaming so that a court order may be sought for a tap on the appropriate roaming switch; and
- It recognizes that no cause of action should be assessed against carriers for the failure of manufacturers or support service providers to develop software or hardware necessary to enable carriers to comply with the capability requirements of the Act.

### B. TECHNICAL REQUIREMENTS AND SOLUTIONS

#### 1. Electronic Surveillance Needs of Law Enforcement

IN JULY 1992, THE FEDERAL BUREAU OF INVESTIGATION, in cooperation with other federal, state and local law enforcement agencies, identified nine technical needs that must be met in order for law enforcement to successfully conduct court-authorized surveillance of electronic communications.<sup>1</sup> According to law enforcement authorities, they require:

1. Access to call content and call setup information<sup>2</sup> going to and from an intercept subject within a service area operated by service providers served with a court order authorizing electronic surveillance;
2. Real-time, full-time monitoring capability for intercepts;
3. Transmission of intercepted communications by service providers to remote monitoring facilities designated by law enforcement;
4. Transparency of interception-related activities to unauthorized parties, including intercept subjects, and implementation of safeguards by carriers to restrict access to intercept information;
5. Verifying information supplied by carriers which associates intercepted communications with intercept subjects, and information on services and features subscribed to by intercept subjects;
6. Increased capacity for implementing a number of simultaneous intercepts;
7. Expeditious access to the communications of intercept subjects;
8. Reliability of intercept service comparable to the reliability of service provided to intercept subjects; and
9. Quality of intercept transmissions forwarded to monitoring facilities consistent with all performance standards of the service provider.

### 2. Electronic Communications Service Provider Committee

IN MARCH 1993, THE ELECTRONIC COMMUNICATIONS SERVICE PROVIDER (ECSP) COMMITTEE was created by the Alliance for Telecommunications Industry Solutions (ATIS, formerly the Exchange Carrier Standards Association) in response to a request from the telecommunications industry and law enforcement that ATIS sponsor a committee to identify, and develop solutions to, technical and associated operational issues surrounding court-authorized electronic surveillance. The ECSP Committee is comprised of representatives of Regional Bell Operating Companies, interexchange carriers, wireless service providers, independent local exchange carriers, industry associations, telecommunications equipment manufacturers and law enforcement agencies. Each subcommittee of the ECSP is co-chaired by a committee member from industry and a committee member from law enforcement.

In furtherance of its mission, the ECSP Committee established a Wireless Cellular Action Team to address issues involving technical capabilities for the surveillance of electronic communications within cellular communications systems. Since its creation, this action team has examined existing cellular intercept features and evaluated the ability of these features to satisfy the needs and requirements of law enforcement for electronic surveillance. The ECSP has also created an action team focusing on the technical requirements of PCS systems.

### 3. Issues of Continuing Concern

CTIA CONTINUES TO WORK WITH LAW ENFORCEMENT, THE INDUSTRY, AND CONGRESS to resolve issues arising out of implementation of the new law. To that end, some carriers have expressed con-

cern regarding the definition of "call-identifying information" which contemplates cell site or location-related information (see § 103 (a)(2)(B)), and the provision that states that a pen register order or trap and trace order may not obtain call-identifying information that discloses the physical location of the subscriber (see § 103 (a)(2)(B)). These sections may suggest that reasonable cause, the legal showing necessary to obtain a pen register or trap and trace order, is insufficient to obtain location-related information. Instead, parties may have to prove probable cause, the highest level of proof, which is necessary for an eavesdropping or search warrant.

THE ACT CONSISTS of the following three titles:

- Title I adds chapter 120 to Title 18 and is composed of twelve sections, including the wiretap capability and capacity requirements.
- Title II expands the privacy protection of the Electronic Communications Privacy Act to cover cordless telephones and certain radio-based communications; prohibits the fraudulent alteration of commercial mobile radio instruments; requires a court order for the disclosure of transactional data on electronic communications services; limits the use of pen registers that intercept information other than dialing or signalling information; and makes other technical changes.
- Title III amends the Communications Act of 1934 by requiring the FCC to prescribe rules for implementing the Act's systems security and integrity requirements, by authorizing common carriers to petition the FCC to adjust charges to recover costs of compliance, and by making certain clerical and technical amendments and eliminating expired and outdated provisions of the communications laws.

### III. Relevant Section Analysis

#### A. Coverage and Scope, Section 102

IN 1968, CONGRESS PASSED "THE WIRETAP ACT," codified at chapter 119, 18 U.S.C. §§ 2510-21, as amended, that made the government's surveillance activities lawful and set up a judicial process to which law enforcement must adhere in order to obtain court-ordered wiretap authority. In response to evolving computer and telecommunications technology, the Electronic Communications Privacy Act was passed in 1986. This law amended the 1968 Wiretap Act by protecting a new class of electronic communications, including cellular telephones, paging devices, electronic mail, and computer databases. In addition, for the first time, the "technical assistance" responsibility was outlined directing telecommunications providers and other persons to furnish "all information, facilities, and technical assistance necessary" to accomplish a surveillance permitted by law.<sup>3</sup>

Public Law 103-414, the "Communications Assistance for Law Enforcement Act" adds, among other things, chapter 120 to Title 18, United States Code, defining in more detail the technical assistance that telecommunications carriers are required to provide in connection with court orders for wire and electronic interceptions, pen registers, and trap and trace devices. The intent is to make more certain the duty of telecommunications carriers to cooperate in the lawful interception of communications for law enforcement purposes.

Telecommunications carriers are required to have sufficient capacity to execute all electronic surveillance orders and to provide the following capabilities: (1) to expeditiously isolate the content of targeted commu-

nications transmitted within the carrier's service area; (2) to expeditiously isolate call-identifying information providing the origin and destination of targeted communications; (3) to deliver intercepted communications and call-identifying information to lines or facilities leased by law enforcement for transmission to a location away from the carrier's premises, concurrently with transmittal of the communications to or from the subscriber; and (4) to do so unobtrusively, so the targets of surveillance are not made aware of the lawful interception.

The term "telecommunications carrier" is defined, for purposes of this Act, as "any person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service, as defined in section 332(d) of the Communications Act." This definition encompasses local exchange carriers, interexchange carriers, competitive access providers, wireless carriers (including cellular, PCS, and satellite providers), cable companies that offer telephony, and any other common carrier who offers wireline or wireless services for hire to the public. The definition does not cover information services, such as electronic mail providers, online services providers, or commercial Internet providers. It also does not include persons or entities engaged in providing call forwarding services, speed dialing, or the call redirection portion of a voice mail service.

In keeping with the expected increase of competitive providers of local exchange service, the FCC is authorized to designate other persons and entities as telecommunications carriers subject to the Act's assistance requirements in section 103 to the extent that such person or entity serves as a replacement for the local telephone service to a substantial portion of the public within a state and such designation is in

### III. Relevant Section Analysis, Continued

the public interest. As part of its determination regarding the public interest, the Commission shall consider, among other things, whether it would promote competition, encourage the development of new technologies, and protect public safety and national security. In addition, the FCC is authorized, after consultation with the Attorney General, to exempt classes or categories of telecommunications carriers from the Act's coverage.

The scope of the assistance requirement imposed upon carriers is consistent with existing law which imposes a duty to furnish all necessary assistance pursuant to 18 U.S.C. § 2518(4). However, it is limited in several ways. First, law enforcement agencies may not dictate the specific design of systems or features, nor prohibit the adoption of any design by carriers. Further, as long as each communications message can be intercepted by at least one method, the Act leaves to the industry how to accomplish compliance. Moreover, telecommunications carriers are not required to decrypt encrypted communications that are the subject of the court-ordered wiretap, unless the carrier provided the encryption service and can decrypt the communication.

#### **B. Mobile Service Assistance Requirement, Section 103(d)**

WHEN A TARGETED SUBSCRIBER'S CALL CONTENT AND CALL-IDENTIFYING information originate outside a wireless carrier's service area, that carrier is no longer responsible for the delivery of the intercepted communications. Under such circumstances, the carrier is only responsible for notifying law enforcement as to which carrier or service provider has subsequently begun serving the target.

#### **C. Capacity Requirements, Section 104**

THE SECTION ENTITLED "NOTICE OF CAPACITY REQUIREMENTS" places upon the government the burden to estimate its capacity needs in a cost-efficient manner, while also providing carriers with a "safe harbor" for capacity. Within one year of enactment, *i.e.*, October 25, 1995, the Attorney General, after notice and comment, must publish in the Federal Register and provide to appropriate industry associations and standard-selling bodies both the maximum capacity and initial capacity required to accommodate all intercepts, pen registers, and trap and trace devices that all levels of the government expect to operate simultaneously. The maximum capacity relates to the greatest number of intercepts a particular switch must be capable of implementing simultaneously. Conversely, the initial capacity relates to the number of intercepts the government will need to operate upon the date of enforcement of this Act, *i.e.*, four years from the date of enactment.

The Attorney General is directed to develop the notices after consultation with local and state law enforcement authorities, the carriers, equipment manufacturers, and manufacturer support service providers. The Attorney General is given flexibility to determine the form of the notice; *i.e.*, the notice may be based on the type of equipment, type of service area, nature of the service area, or any other measure. The notice must identify, to the maximum extent practicable, the capacity required at specific geographic locations.

Subject to the reimbursement conditions, telecommunications carriers must ensure that, within three years after publication of the notice or four years after enactment, whichever is longer, they have the initial and

### III. Relevant Section Analysis, *Continued*

the maximum capacity to execute all surveillance orders. The Attorney General has one year, after enactment, in which to notify carriers of the government's capacity needs. If the Attorney General publishes the first capacity notice before the statutory time period of one year has elapsed, carriers must satisfy the capacity requirement by October 25, 1998, the effective implementation date of the law. However, in the event the Attorney General publishes the capacity notices after the statutory one-year deadline, carriers have three years thereafter to comply, which time period will fall after the effective date of the Act.

The Attorney General may periodically give written notice to covered entities of any necessary increases in maximum capacity. Carriers will have at least three years, and up to any additional time beyond three years as agreed to by the Attorney General, to comply with the increased maximum capacity requirements.

#### **D. Enforcement Orders, Section 108**

THE ACT PROVIDES FOR ENFORCEMENT BY THE COURTS. A court order may be issued upon the following grounds. First, the court must find that law enforcement has no reasonably achievable alternatives for implementing the order through the use of other technologies or capabilities, or by serving the order on another carrier or service provider. Essentially, the court must find that law enforcement is seeking to conduct its interception at the best, or most reasonable, place for such interception.

Second, the court must find that compliance with the requirements of the Act is reasonably achievable through application of available technology, or would have been reasonably achievable if timely action had

been taken. A determination of "reasonably achievable" involves a consideration of economic factors. This limitation is intended to excuse a failure to comply with the assistance capability requirements or capacity notices where the total cost of achieving compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features. In addition, this provision recognizes that, in certain circumstances, telecommunications carriers may deploy features or services even though they are not in compliance with the requirements of this Act.

In the event that either of these grounds is not met, the court may not issue an enforcement order and the carrier may proceed with the deployment, or continued offering to the public, of the equipment, facility, or service at issue.

If conditions are met for issuance of an enforcement order, the court must set a reasonable time and conditions for complying with its order. In determining what is reasonable, the court may consider, on a case-by-case basis, several enumerated factors.

The court's authority to issue enforcement orders is limited by three situations. First, an enforcement order may not be issued requiring a carrier to exceed the capacity set forth in the Attorney General's notices, issued pursuant to §104 of the Act.

Second, an enforcement order may not require a carrier to comply with the assistance capability requirements if the FCC has determined, pursuant to its authority under §109(b)(1), that such compliance is not reasonably achievable. However, if the Attorney General agrees to pay the incremental costs to make compliance reasonably achievable, pursuant to §109(b)(2), this limitation does not apply.



### III. Relevant Section Analysis, *Continued*

Finally, an enforcement order may not require a carrier to modify equipment, facilities, or services deployed before January 1, 1995, to comply with the assistance capability requirements, unless the Attorney General has agreed to pay for all reasonable costs directly associated with the modifications necessary for compliance. However, if such non-compliant equipment, facilities, or services are replaced, significantly upgraded or otherwise subjected to major modification after January 1, 1995, this limitation again does not apply.

#### **E. Appropriations and Cost Reimbursement, Sections 109 and 110, respectively**

THE ACT AUTHORIZES \$500,000,000 TO BE APPROPRIATED for fiscal years 1995 through 1998 to carry out its purposes, and requires the Attorney General to pay all reasonable costs directly associated with modifications to pre-existing equipment, facilities, or services, *i.e.*, those equipment, services, or facilities deployed before January 1, 1995.

For equipment, facilities, or services that are deployed after January 1, 1995, the Act authorizes telecommunications carriers and other interested persons to petition the FCC for a determination of whether compliance with the assistance capability requirements is reasonably achievable. The FCC is given one year after the petition is filed to make its determination. In reaching its decision, the FCC is directed to determine if compliance would impose significant difficulty or expense on the carrier or users, and to consider a number of enumerated factors, including the effect on public safety and national security, the rates for basic residential telephone service, and the need to protect the privacy and security of communications not authorized to be intercepted.

If compliance with the assistance capability requirements is not reasonably achievable for equipment, facilities, and services deployed after January 1, 1995, the Attorney General is authorized, upon application by a carrier, to agree to pay additional reasonable costs to make compliance reasonably achievable. If the Attorney General elects not to pay, the equipment, feature or service in question will be considered in compliance, until it is replaced, significantly upgraded or otherwise undergoes major modifications in the ordinary course of business.

Additionally, the Attorney General is authorized, after notice and comment, to establish regulations to effectuate the timely and cost-efficient processing of any payment from the government to carriers under this Act, pursuant to chapters 119 and 120 of Title 18 of the U.S. Code, and under the Foreign Intelligence Surveillance Act of 1978. The Attorney General is further directed to consult the FCC about issuing regulations to determine reasonable costs. Such regulations must minimize the cost to the federal government and maintain the confidentiality of trade secrets, while permitting recovery from the government of (i) the direct research and development costs that have not been recovered from any other governmental or non-governmental entity, (ii) the direct costs attributable to compliance with the Act for personnel training and the deployment or installation of equipment or facilities, and (iii) in case of modifications that may be used for purposes other than for lawfully authorized electronic surveillance, only the incremental costs attributable to compliance. Such regulations will require telecommunications carriers to submit to the Attorney General claims for payment and such other information as she may require.

### III. Relevant Section Analysis, *Continued*

THE EFFECTIVE DATE FOR COMPLIANCE with the assistance capability requirements in section 103 and the systems security and integrity requirements in section 105 is set at four years after enactment, *i.e.*, October 25, 1998. All other provisions took effect upon the date of enactment, *i.e.*, October 25, 1994.

#### **End notes:**

1. The nine requirements originally identified by law enforcement in 1992 have since been reviewed by the telecommunications industry and clarified by law enforcement. They are discussed in detail in the document entitled "Law Enforcement Requirements for the Surveillance of Electronic Communications" issued in June 1994. To obtain a copy, please contact the Department of Science and Technology at CTIA.
2. "Call setup information" is the Mobile Telephone Switching Office's (MTSO's) resident internal data that is used to establish a link to the cellular subscriber. This information contains: (1) call destination (dialed digits); (2) identity of the location of the incoming call; (3) date, time, and duration of the call; and (4) first and/or last cell site used to deliver the call. "Call content information" is the content of the call (the conversation or the data transmitted during the call).
3. See, 18 U.S.C. §§ 2518(4), 3124; see also 50 U.S.C. §1802(a)(4).

**PUBLIC LAW 103-414**  
**"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"**

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
<b>FRAUDULENT ALTERATION OF CMRS INSTRUMENTS</b>	Effective upon date of enactment, <i>i.e.</i> , October 25, 1994 see Title II, §206.	<p>Offense: It is unlawful to knowingly and with intent to defraud use, produce, or traffic in, have control or custody of, or possess a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; or knowingly and with intent to defraud use, produce, or traffic in, have custody or control of, or possess a scanning receiver, or hardware or software for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services.</p> <p>Title II, §206(a); see also Title 18, U.S.C. §1029(a) (5)-(6).</p> <p>Penalty: The fines pursuant to the alteration of telecommunications instruments and equipment are not more than the greater of \$50,000 or twice the value obtained by the offense, or imprisonment for not more than 15 years, or both in the case of an offense involving the fraudulent alteration of a telecommunications instrument which does not occur after a conviction for another offense or an attempt to commit another offense under this subsection.</p> <p>Title II, §206(b); see also Title 18, U.S.C. §1029(c)(2).</p> <p>Definitions: The term "access device" now includes electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier.</p> <p>Title II, §206(c)(1); see also Title 18, U.S.C. §1029(e)(1).</p> <p>In addition, the term "scanning receiver" is defined as "a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119."</p> <p>Title II, §206(c)(4); see also Title 18, U.S.C. §1029(e)(7).</p>	Not applicable.	Not applicable.

**PUBLIC LAW 103-414**  
**"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"**

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
<b>SCOPE OF COVERAGE</b>	Effective upon date of enactment, i.e., October 25, 1994. Title I, §111(a).	Any person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, including CMRS providers, and providers of wire or electronic communication switching or transmission service that the FCC finds is a replacement for a substantial portion of the local exchange service and where public interest would be served to deem those entities covered. Title I, §102(8)(A)-(B)(i)-(ii)	See, <i>infra</i> , capability requirements.	"Telecommunications carrier" does not include persons or entities engaged in providing information services; and any class or category of telecommunications carriers that the FCC exempts by rule after consultation with the Attorney General (AG). Title I, §102(8)(C)(i) (ii), see also, Title I, §103(b)(2)(A) (B).
<b>MOBILE SERVICE ASSISTANCE</b>	Effective 4 years after date of enactment, i.e., October 25, 1998. Title I, §111(b)	CMRS providers offering features or services that allow subscribers to redirect, hand off, or assign their communications to another service area or provider must ensure that when they no longer have access to the content or call-identifying information within the service area where the interception has been occurring, the CMRS carrier must provide the government with the identity of the carrier that has acquired the communication before, during, or immediately after the transfer of the communication. Title I, §103(d).	See, <i>infra</i> , capability requirements.	
<b>INFORMATION SERVICES AND PRIVATE NETWORKS</b>	Not applicable.	Not applicable.	Not applicable.	The capability requirements do not apply to information services or private networks that provide transport, switching facilities or solely provide interconnection services. Title I, §103(b)(2)(A) (B), see also, Title I, §102(8)(C)(i) (ii)

**PUBLIC LAW 103-414**  
**"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"**

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
<b>CAPACITY</b>	<p>Effective upon date of enactment, <i>i.e.</i>, October 25, 1994.  Title I, §111(a)</p> <p>Notices of Maximum and Actual Capacity Requirements: Not later than 1 year after the date of enactment (<i>i.e.</i>, October 25, 1995), and after consulting with state and local law enforcement agencies, carriers, manufacturers and support service providers, and after notice and comment, the AG must publish in the <u>Federal Register</u> and provide to industry associations and standard-setting bodies notice of the actual and maximum number of interceptions, pen registers, and trap and trace devices that the government estimates to use simultaneously by the date that is 4 years after the date of enactment, <i>i.e.</i>, October 25, 1998. Title I, §104(a)(1)(A)-(B).</p> <p>Carrier Compliance Date. Within 3 years after notice of capacity is published (October 25, 1997) or within 4 years after the date of enactment (October 25, 1998), whichever is longer.  Title I, §104(b)(1)-(2).</p> <p>Notices of Increased Maximum Capacity Requirements: The AG must publish in the <u>Federal Register</u>, after notice and comment, notice of any necessary increases in the maximum capacity requirement set forth in the notice pursuant to Title I, §104(c)(1).</p>	<p>Initial Capacity: Carriers must ensure, subject to the availability of appropriations, that their systems are capable of accommodating simultaneous interceptions, pen registers, and trap and trace devices, and able to expand to its maximum capacity requirements.  Title I, §104(b)(1)(A)-(B).</p> <p>Expansion to Maximum Capacity: After the time set for compliance with initial capacity requirements, and subject to the availability of appropriations, a carrier must ensure that it can accommodate expeditiously any increase in the actual number of interceptions, pen registers, and trap and trace devices, up to the number set forth in the maximum capacity notices. Title I, §104(b)(2).</p> <p>Basis of Notices: Notice of capacity requirements may be based on the type of equipment, type of service, number of subscribers, type or size of carriers, nature of service area, or any other measure, and must specify, to the extent practicable, the capacity required at specific geographic locations. Title I, §104(a)(2).</p> <p>Carrier Statement: Within 180 days (6 months) after publication of the capacity notices by the AG, carriers must submit a statement identifying any of its systems or services that do not have the capacity to accommodate simultaneous interception, pen register, and trap and trace device orders. Title I, §104(d).</p> <p>Compliance With Notices of Increased Maximum Capacity: Within 3 years after notice of increased maximum capacity requirements is published, or within such longer time period as the AG may specify, a carrier must ensure that its systems are capable of expanding to the increased maximum capacity set by the notice.  Title I, §104(c)(2).</p>	<p>The AG must review the statements submitted pursuant to §104(d) and, subject to the availability of appropriations, may agree to reimburse the carrier for costs directly associated with the capacity modifications/upgrades submitted for review. Until the AG agrees to reimburse the carrier, the carrier will be considered in compliance with the actual or maximum capacity notices.  Title I, §104(e).</p>	

**PUBLIC LAW 103-414**  
**"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"**

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
<b>CAPABILITY</b>	Effective 4 years after date of enactment, i.e., October 25, 1998. Title I, §111(b).	<p>Pursuant to a court order or lawful authorization, carriers must ensure that their equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of:</p> <p>(1) expeditiously isolating (to the exclusion of all other communications) and enabling the government, concurrently with its transmission, to intercept communications, within its systems;</p> <p>(2) expeditiously isolating and enabling the government to access call-identifying information that is reasonably available to the carrier before, during, or immediately after transmission, and which allows the call-identifying information to be associated with the communication to which it relates;</p> <p>(3) delivering intercepted communications and call-identifying information in a format that may be transmitted by the government to a location away from the carrier's premises; and</p> <p>(4) unobtrusively providing interceptions and access to call-identifying information with a minimum of interference to the subscriber's service and which protects the privacy and security of the communications.</p> <p>Title I, §103(a)(1)-(4)</p> <p>Cost Recovery for Compliance: A carrier may petition the Commission to adjust charges, and regulations to recover costs expended for making capability modifications to equipment, facilities, or services pursuant to requirements of this Act. Title III, §301; see also 47 U.S.C. §229(e)(1).</p>	<p>Equipment, Facilities, and Services Deployed On or Before January 1, 1995: AG may, subject to the availability of appropriations, agree to pay carriers for all reasonable costs directly associated with modifications to be made. Title I, §109(a).</p> <p>Equipment, Facilities, and Services Deployed After January 1, 1995: On petition from carriers, and after notice to the AG, the FCC must determine whether carrier capability compliance is "reasonably achievable." Title I, §109(b).</p> <p>Determinations of Reasonably Achievable for Equipment, Facilities, and Services Deployed After January 1, 1995: Within 1 year after the date the petition is filed, the FCC must decide whether compliance would impose significant difficulty or expense on the carrier or the users of its systems. Additional factors may be considered such as, including, but not limited to: the impact on public safety and national security, rates for basic residential telephone service; privacy protections; the need to achieve the capability requirements by cost-effective methods; the effect on the operation of the equipment, facility, or service at issue; the effect on the nature and cost of the equipment, facility, or service at issue; the U.S. policy to encourage the provision of new technologies and</p> <p>(Continued On Next Page)</p>	<p>Law enforcement agencies or officers are not authorized to require specific design or prohibit the adoption of equipment, services, or features. Title I, §103(b)(1)(A)-(B).</p> <p>An enforcement order shall not require a carrier to modify, for the purposes of complying with the capability requirements, any equipment, facility, or service deployed on or before January 1, 1995 unless the AG has agreed to pay the carrier for all reasonable costs associated with the modifications necessary to bring equipment, facilities, or services into compliance; or the equipment, facility, or service has been replaced or significantly upgraded or otherwise has undergone major modifications. Title I, §108(c)(3)(A)-(B).</p>

**PUBLIC LAW 103-414**  
**"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"**

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
CAPABILITY, continued			<p>services to the public; the financial resources of the carrier; privacy protections; competitive effect on the offering of new equipment, features, and services; and other factors as determined by the FCC.  Title I, § 109(b)(1)(A)-(K).</p> <p>Compensation: If the FCC determines that compliance is not "reasonably achievable," the AG may agree, subject to availability of appropriations, to pay the carrier for the additional reasonable costs of compliance with the capability requirements; or, if the AG does not agree to the additional costs, the carrier will be deemed in compliance with the capability requirements.  Title I, § 109(b)(2)(A)-(B).</p> <p>Failure to Make Payment for Equipment, Facilities, and Services Deployed On or Before January 1, 1995: If a carrier has requested payment, and the AG has not agreed to pay the carrier for all reasonable costs directly associated with the modifications to bring any equipment, facility, or service deployed on or before the enactment date, such equipment, facility, or service will be considered in compliance with the capability requirements until the equipment, facility, or service is replaced or substantially upgraded or otherwise modified.  Title 18, § 109(d).</p>	

**PUBLIC LAW 103-414**  
**"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"**

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
<b>SYSTEMS SECURITY AND INTEGRITY</b>	Effective four years after the date of enactment, i.e., October 25, 1998. Title I, §111(b).	A carrier must ensure that any interception of communications or access to call-identifying information effected within its switching premises be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee acting in accordance with regulations set by the FCC. Title I, §105.		
<b>FCC AUTHORITY TO ENFORCE COMPLIANCE</b>		The FCC must prescribe rules implementing the requirements of this Act, which shall include systems security and integrity rules that require carriers to: establish appropriate policies and procedures for the supervision and control of their officers and employees to activate interception of communications or access to call-identifying information, and prevent any intervention or access without such authorization; maintain secure and accurate records of any interceptions or access; and to submit to the FCC the policies and procedures adopted to comply. Title III, §301; <del>see also</del> . 47 U.S.C. §229(b)(1)-(3).  The FCC must review the policies and proce- dures submitted pursuant to 47 U.S.C. §229(b)(3) and shall order a carrier to modify any policy or procedure that does not comply with FCC regulations. The FCC shall conduct investigations as necessary to insure carrier compliance with these regulations. Title III, §301; <del>see also</del> . 47 U.S.C. §229(c).		



**PUBLIC LAW 103-414**  
**"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"**

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
<p><b>ALLOCATION OF FUNDS FOR PAYMENT</b></p>	<p>Effective upon date of enactment, i.e., October 25, 1994  Title I, §111(a).</p>	<p>Allocation of Funds: The AG must allocate appropriated funds to carry out the bill's requirements in accordance with law enforcement priorities as determined by the AG.  Title I, §109(c).</p> <p>Authority for Appropriations: A total of \$500,000,000 (\$500 million) is authorized to be appropriated to carry out the obligations of the Act for fiscal years 1995-1998. Such sums are authorized to remain available until expended.  Title I, §110.</p> <p>Cost Control Regulations: After notice and comment, the AG must establish regulations necessary to effectuate timely and cost-efficient payment to carriers.  Title I, §109(e)(1).</p> <p>Content of Regulations: The AG, after consultation with the FCC, must prescribe regulations to determine the reasonable costs associated with this Act. The regulations must seek to minimize the cost to the Federal Government and must permit recovery from the Federal Government of: (1) direct costs of developing the capability modifications, or providing requested capacities, but only to the extent that such costs have not been recovered from any other governmental or non-governmental entity; (2) the costs of training personnel in the use of the capabilities and capacities; and (3) the direct costs of deploying or installing such capabilities and capacities.  Title I, §109(e)(2)(A)(i)-(iii).</p> <p>In the case of any modification that may be used for any purpose other than to execute a lawfully authorized surveillance order, the AG may permit recovery of only the incremental cost of making the modification suitable for law enforcement purposes.  Title I, §109(e)(2)(B).</p>		